Amendments to the Specification

Replace the paragraph beginning at page 5, line 8 with:

While the appended claims set forth the features of the present invention with particularity, the invention, together with its objects and advantages, may be best understood from the following detailed description taken in conjunction with the accompanying drawings of which:

Figure 1 is a block diagram generally illustrating an exemplary computer system on which the present invention may be implemented;

FIG. 2 is a schematic diagram illustrating a mobility support scheme for a mobile device in accordance with an embodiment of the invention;

FIG. 3 is a schematic diagram showing an implementation of the mobility support scheme of FIG. 2;

FIGS. 4A and 4B are schematic diagrams showing an example of the contents of security filters and TCP control blocks of a mobile host and a correspondent host before and after an address change of the mobile host; ~~and~~

FIG. 5 is a schematic diagram showing the format of the data packets being tunneled between the mobile host and the correspondent host for handling the address change of the mobile device[[.]];

FIG. 6 is a flowchart depicting steps performed by a mobile host in accordance with an embodiment of the invention; and

FIG. 7 is a flowchart depicting steps performed by a correspondent host in accordance with an embodiment of the invention.

Replace the paragraph beginning at page 12, line 5 with:

When the mobile host 70 changes to a new address, the networking stack of the mobile host deprecates the old address (see Step 602 at Fig. 6). The mobility service 100 of the mobile host then sends an address change notification message (ACM) 102 to each correspondent host 72 that has a connection with it over a secured control channel 96 established with that correspondent host (see Step 608 at Fig. 6).

Replace the paragraph beginning at page 12, line 18 with:

The mobility service 100 of the mobile host then sends an address change notification message 102 through the tunnel to each correspondent host 72 that has a connection with it over the secured control channel 96 established with that correspondent host. The address change notification message 102 contains the mobile host's new address. When the correspondent host 72 receives the address change message 102 (see Step 702 at Fig. 7), it authenticates the message based on security filters 88 set up for the existing connection with the mobile host 70 to verify that the message is indeed from the mobile host. At this point, the security filters 88 on the correspondent host still use the old address of the mobile host, and the tunneling of the message 102 allows the message headers, such as the IP header and the TCP or UDP headers, to pass (i.e., match) the security filters and the transport control parameters in the same way as packets sent by the MH prior to the address change.

Replace the paragraph beginning at page 13, line 8 with:

After authenticating the address change notification message 102, the mobility service 106 of the correspondent host sends an acknowledgment message 108 to the mobile host 70 (see Step 704 at Fig. 7). Like the notification message, the acknowledgment 108 is also tunneled so that it will pass/match the security filters 82 and Transport Control parameters on the mobile host, which are still using the old address of the mobile host. The mobility service 106 of the correspondent host then modifies the security filters 88 (see Step 710 at Fig. 7) and transport control parameters 92 (see Step 712 at Fig. 7) for the connection 78 to use the new address of the mobile host instead of the old address. Thus, any new packets from the application 76 to the mobile host will be sent to the new address of the mobile host. The security association 86 for that connection is otherwise kept the same as before the address change.

Replace the paragraph beginning at page 13, line 23 with:

Upon receiving and authenticating the acknowledgment 108 (see Step 610 at Fig. 6), the mobility service 100 of the mobile host modifies the security filters 82 (see Step 612 at Fig. 6) and transport control parameters 90 (see Step 614 at Fig. 6) for the connection 78 with the correspondent host. As a result of the changes by the mobility services 100 and 106 of the mobile host and the correspondent host, the communication connection 78 between the two hosts has been "migrated" from the old address of the mobile host to the new address. All subsequent traffic between the mobile host and the correspondent host is sent over the migrated connection, while being secured by the same security associations 86 and 84 used prior to the migration. The migration of the connection is transparent to the applications 74 and 76 that communicate over the connection before, during, and after the handling of the address change. In other words, the applications do not have to be aware of the address change. To them, the connection is always there and the communications are sent through the connection regardless of any address change.

Replace the paragraph beginning at page 20, line 15 with:

Since the old address is deprecated, the IP routing entries 162 corresponding to it are removed from the IP routing table 164 of the mobile host (see Step 604 at Fig. 6). An IP-in-IP tunneling entry 166, however, is created by the mobility service in their place (see Step 606 at Fig. 6). There is one tunneling entry for the old address in place of all earlier entries for the old address in the routing table. This tunnel is created for encapsulating packets that are sent with the old IP address of the mobile host as the source address. Due to the new tunneling entry in the IP routing table, such packets are tunneled. The data structure of such a tunneled packet 170 is shown in FIG. 5. This packet is generated from the original packet by adding an outer IP header 172 that contains the new IP address of the mobile host as the source address, while an inner IP header 176 contains the old address as the source address.

Replace the paragraph beginning at page 22, line 9 with:

When the ACM packet 192 reaches the correspondent host, the correspondent host's TCP/IP stack de-tunnels the packet and then authenticates it as part of normal IPSEC processing. As mentioned above, the IPSEC implementation provides the secured control channel for delivering the address change notification from the mobile host. Once authenticated, the packet is delivered to the OAKLEY service 200 on the correspondent host. The OAKLEY service 200 extracts the security association ID and the old and new IP addresses of the mobile host from the packet, and creates and IP-in-IP tunneling entry in the IP routing table 202 based on the pair of old and new addresses (see Step 706 at Fig. 7).

Replace the paragraph beginning at page 22, line 21 with:

The OAKLEY service 200 then sends a "MIGRATION COMPLETED" ISAKMP NOTIFY message 206 to the old mobile host address. This acts as an acknowledgment to the address change notification message 192 sent by the mobile host. This acknowledgement (ACK) packet 206 is secured by IPSEC under the ISAKMP SA existent for the old address of the mobile host. This packet 206 is tunneled to the mobile host. As shown in FIG. 5, due to the tunneling, the packet 206 is encapsulated such that its outer IP header 208 carries the new mobile host address as the destination address and the inner IP header 210 carries the old mobile host address as the destination address. Returning again to FIG. 3, in addition to sending the acknowledgment packet 206, the OAKLEY service 200 on the correspondent host delivers a "CHANGE FILTERS" PnP event notification to the IPSEC driver 140. This event contains the new address of the mobile host 120. Upon getting the PnP event from the OAKLEY service 200, the IPSEC driver 140 modifies the filters 136 for all the security associations with the mobile host to use the new mobile host address instead of the old one. The OAKLEY service 200 further delivers a "CHANGE TCB" PnP event to the TCP/IP driver 204. In response, the TCP/IP driver 204 changes the TCBs 150 corresponding to the mobile host to use the new address of the mobile host. Once the TCBs 150 are modified, the OAKLEY service 200 tells the IP driver 218 to remove the tunneling entry for the old mobile host address from the routing table 202 (see Step 708 at Fig. 7), as it is no longer needed since all new packets to the mobile host will be addressed to the new mobile host address according to the modified TCBs.